Perbandingan Kriptografi Visual dengan Penyembunyian Pesan Gambar Sederhana *Adobe Photoshop*

Risalah Widjayanti - 13509028
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509028@std.stei.itb.ac.id

***Abstract*—Kriptografi visual adalah cara menyembunyikan pesan gambar sedemikian rupa sehingga dekripsinya dapat dilakukan secara langsung tanpa bantuan komputer. Akan tetapi, cara ini memiliki beberapa kelemahan yang menyulitkan pihak pendekripsi maupun memberi keuntungan pada kriptanalis.**

Ide makalah ini adalah membandingkan penyembunyian gambar sesuai dengan ketentuan yang ada dalam kriptografi visual dengan penyembunyian gambar lewat bantuan perangkat lunak pengolah gambar seperti *Adobe Photoshop*. Makalah ini membahas perbandingan keduanya ditinjau dari sisi kemudahan enkripsi, hasil enkripsi-dekripsi, kemudahan dekripsi, dan tingkat kesulitan pemecahannya.

Index Terms*—*kriptografi visual, image manipulation

I. PENDAHULUAN

Adobe Photoshop boleh jadi perangkat lunak pengolah gambar paling populer yang banyak digunakan untuk mengedit dan memanipulasi gambar. Perangkat lunak satu ini memang bukan perangkat lunak yang bisa digunakan dengan mudah oleh semua orang. Fiturnya yang kaya membuat *Photoshop* sulit untuk dikuasai tanpa banyak mengeksplorasi. Tidak banyak yang tahu kalau fitur yang dimiliki oleh *Photoshop* dapat membantu untuk memanipulasi gambar agar citranya dapat disembunyikan.

Namun, cara penyembunyian gambar tidak hanya dapat dilakukan dengan *photoshop*. Ilmu kriptografi sebelumnya telah menemukan teknik kriptografi visual untuk penyembunyian gambar. Bahkan dengan keunggulan khusus: pendekripsinya tidak memerlukan bantuan komputer. Dekripsi hanya dilakukan dengan menumpuk gambar selama pendekripsinya memiliki bahan dekripsi yang diperlukan.

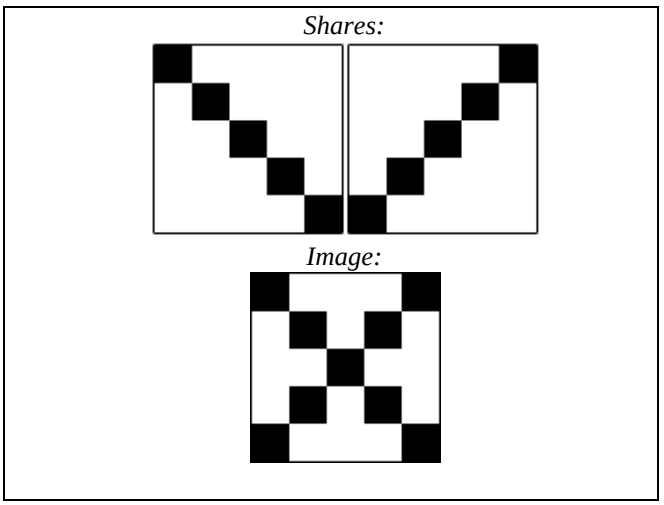
Di tahun 1994, Moni Naor dan Adi Shamir mendemonstrasikan skema rahasia untuk kriptografi visual di mana gambar dibagi menjadi n bagian sehingga hanya seseorang yang memiliki n bagian itu dapat mendekripsikan gambar di mana n-1 bagian tidak akan memberikan informasi apa pun tentang gambar yang sebenarnya. Dekripsinya dilakukan dengan menumpuk gambar yang kesemuanya dijadikan transparan. Ketika seluruh bagian gambar ditumpuk satu sama lain, gambar sebenarnya akan tampak. Sedangkan mengenai skemanya akan dijelaskan lebih lanjut di bab selanjutnya.

II. ENKRIPSI DAN DEKRIPSI KRIPTOGRAFI VISUAL: VISUAL SECRET SHARING (VSS)

Teknik yang diperkenalkan oleh Naor dan Shamir ini pada dasarnya adalah perkembangan berikutnya dari teknik *secret sharing*. Sebuah metode untuk berbagi rahasia kepada anggota grup yang dapat dikonstruksi jika dan hanya jika terdapat sejumlah bagian yang cukup untuk dikombinasikan bersama (bagian yang dimiliki per individu tidak cukup untuk mengetahui apa isi rahasia tersebut). Metode milik Naor dan Shamir ini serupa, intinya setiap *share* (bagian gambar) adalah subset dari gambar yang utuh. Gambar yang utuh tadi dienkripsi dengan memecah belahnya menjadi potongan kecil.

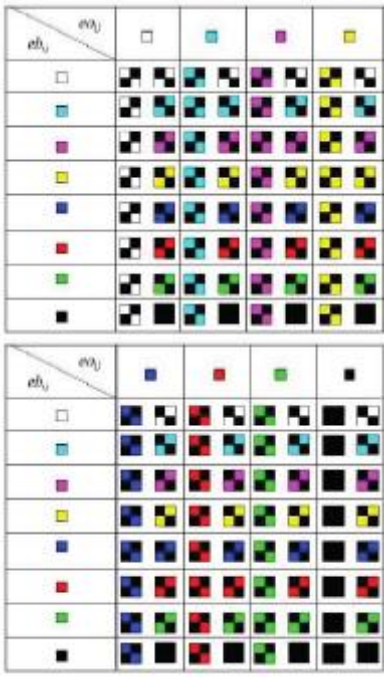
Anggap dalam sebuah gambar berukuran 2x2 pixel berwarna keseluruhan hitam. Gambar tersebut dibagi menjadi empat pixel dengan setiap pixelnya dibagi lagi menjadi n-elemen matriks yang disebut dengan subpixel. Penggabungan n buah subpixel itulah yang nantinya akan menunjukkan di pixel itu bahwa tiap-tiap pixel memiliki warna hitam.

Untuk lebih jelasnya, perhatikan gambar-gambar di bawah ini:



Gambar 1: contoh *share* dan citra asli

Gambar-gambar di atas untuk menunjukkan bagaimana penggabungan pixel membentuk warna hitam dan putih. Sedangkan untuk gambar berwarna, dapat dilihat dari tabel berikut:



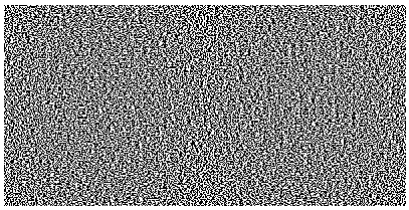
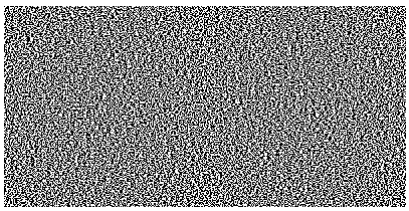
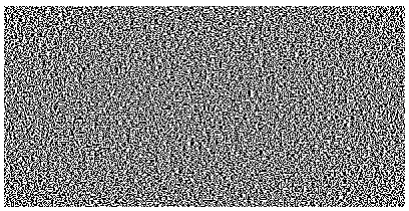
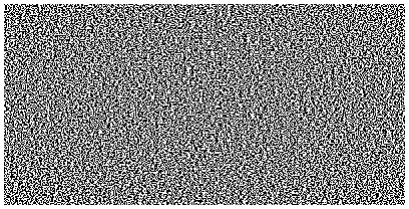
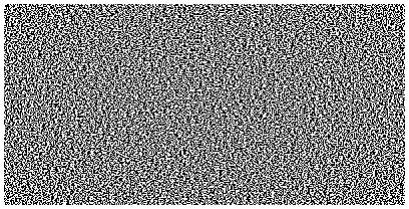
Gambar 2: tabel split warna
Sumber: *Play Color Cipher and Visual Cryptography* (http://www.decisionstats.com/play-color-cipher-and-visual-cryptography/)

Berikut adalah contoh enkripsi dengan menggunakan kriptografi visual. Alat yang digunakan adalah applet VC yang ditulis oleh kepala manajemen keamanan informasi dari Universitas Regensburg. Applet tersebut dapat diunduh di http://www-sec.uni-regensburg.de/vc/.

Gambar asli:

Gambar 3: contoh gambar asli

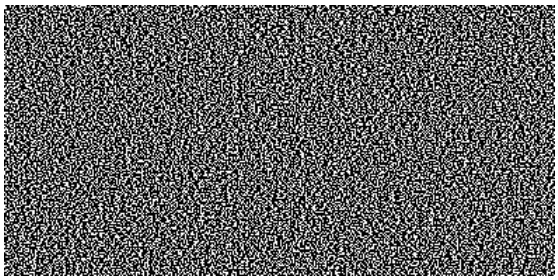
Sharesi:

1. 
2. 
3. 
4. 
5. 

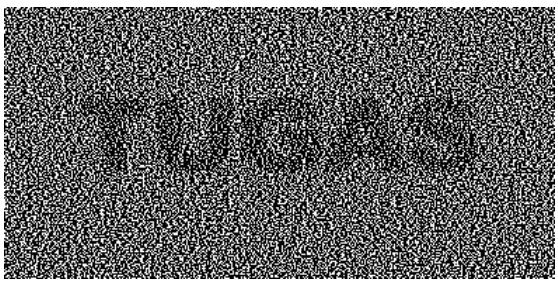
Gambar 4 (1-5): *share* hasil enkripsi gambar 3

Perhatikan bahwa masing-masing citra pada *share* tidak memiliki impresi apa-apa selain *noise* di sana-sini. Hal tersebut bisa saja menimbulkan kecurigaan karena logikanya, orang tidak akan menyimpan sesuatu yang tidak memiliki makna.

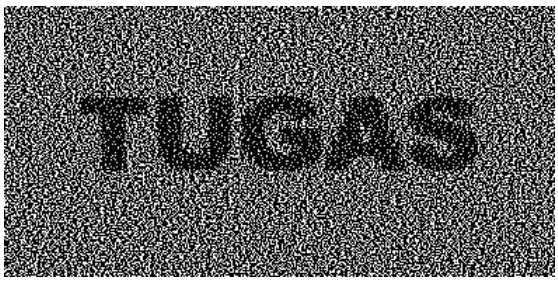
Namun jika gambar tersebut di-*overlay* satu sama lain, barulah dapat memberikan petunjuk citra apa yang ada di sana. Penggabungan subpixel seperti yang telah dijelaskan sebelumnya memutuskan warna pixel apa yang terbentuk untuk gambar hasil dekripsi. Untuk lebih jelasnya, perhatikan rincian berikut:



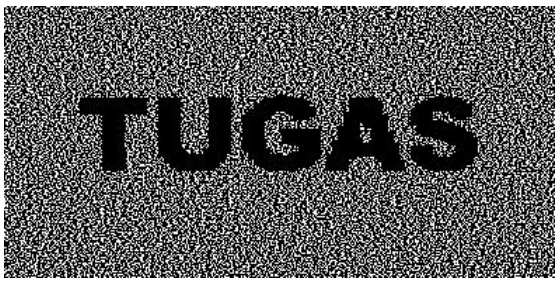
Gambar 5: penggabungan *share* 4.1 dan *share* 4.2



Gambar 6: penggabungan *share* 4.1, *share* 4.2, dan *share* 4.3



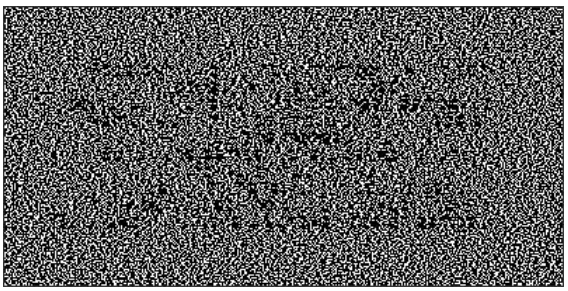
Gambar 7: penggabungan *share* 4.1, *share 4.2, share 4.3, dan share 4.4*



Gambar 8: penggabungan *share* 4.1, *share 4.2, share 4.3, share 4.4, dan share 4.5*

Pada akhirnya, gambar membentuk citraan dengan warna yang tegas bertuliskan kata yang sama dengan gambar asli. Namun yang menjadi masalah di sini adalah *noise* yang mengganggu. Beruntung gambar yang disajikan di atas hanya bitmap dengan tulisan sederhana yang mudah dibaca meskipun dengan *noise* yang cukup *intense.* Bayangkan jika yang digunakan adalah gambar lain.

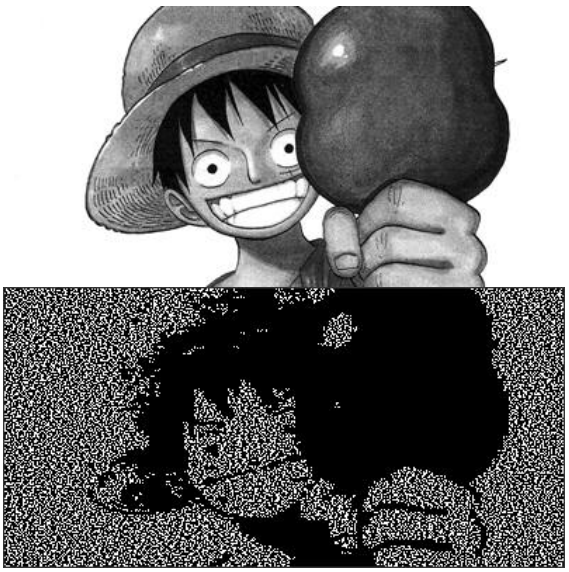
Pada akhirnya, gambar membentuk citraan
dengan warna yang tegas
bertuliskan kata yang sama dengan gambar asli.
Namun yang menjadi masalah di sini adalah
noise yang mengganggu.
Beruntung gambar yang disajikan di atas
hanya bitmap dengan
tulisan sederhana yang mudah dibaca
meskipun dengan noise yang cukup intense.
Bayangkan jika yang digunakan adalah gambar lain.



Gambar 9: contoh satu, gambar asli dan gambar hasil penggabungan seluruh *share* hasil enkripsi

Tulisan setelah didekripsi malah tidak bisa dibaca sama sekali. Karena *noise* hitam putih bercampur dengan hitam putih yang terdapat dalam teks pada gambar asli. Semakin kecil *font* semakin bercampur-baurlah sehingga tidak jelas mana *noise* mana pixel dari teks asli.

Berikutnya dicoba untuk gambar hitam putih. Gambar diambil dari *One Piece* karangan Eiichiro Oda *volume* 62.



Gambar 10: contoh dua, gambar asli dan gambar hasil penggabungan seluruh *share* hasil enkripsi

Gambar hasil dekripsi sudah mengalami penurunan kualitas yang sangat besar. Tidak hanya bercampur dengan *noise*, tapi juga telah kehilangan wujud aslinya sebagai gambar. Dapat dilihat sendiri gambar di atas nyaris tidak dikenali siapa pemilik wajah di gambar tersebut dengan ekspresi dan gerakan yang sulit untuk diraba. Efek cahaya, bayangan, dan gradasi yang ada di gambar sebelumnya lenyap begitu saja karena sudah tercampur dengan *noise.*

Berikutnya dilakukan percobaan dengan menggunakan gambar yang berwarna (sebagai catatan, gambar diambil dari sumber yang sama dengan contoh sebelumnya).

Gambar 11: contoh tiga, gambar asli dan gambar hasil penggabungan seluruh *share* hasil enkripsi

Selain masalah kualitas gambar dan tidak jelasnya hasil dekripsi seperti yang telah dikemukakan sebelumnya, kekayaan warna juga tidak dapat ditampilkan di hasil dekripsi. Dapat dilihat sendiri bahwa warna yang dapat ditampilkan hanya warna dasar RGB (*red, green, blue*)

serta hitam dengan tingkat kecerahan yang rendah karena pixel berwarna hitam mendominasi di *noise*.

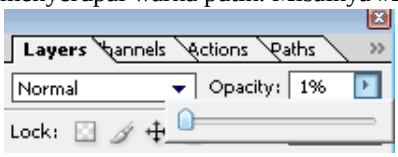
III. PENYEMBUNYIAN GAMBAR DENGAN BANTUAN *ADOBE PHOTOSHOP*

Ada banyak cara yang dapat digunakan untuk menyembunyikan gambar dengan bantuan *Adobe Photoshop*. Namun yang dibahas dalam makalah ini hanya diambil satu cara yang dianggap paling sederhana sehingga lebih mudah untuk dibahas.

Metode ini dapat digunakan untuk file berwarna hitam putih maupun berwarna. Lebih disarankan digunakan untuk warna putih karena gambar berwarna bisa menjadi rusak setelah di-'dekripsi'.

Cara 'enkripsi'-nya sangat sederhana, yakni sebagai berikut:

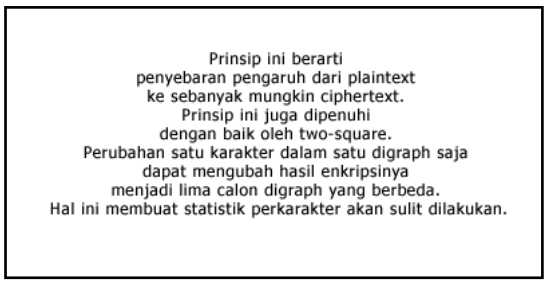
1. Membuat *canvas* baru dengan latar belakang putih
2. Memindahkan *layer* gambar yang ingin disembunyikan ke *canvas* baru tersebut
3. Ubah *opacity* untuk gambar tersebut hingga menjadi 1%. Untuk layer berupa teks, dapat diganti warnanya menjadi font yang menyerupai warna putih. Misalnya #FEFEFE

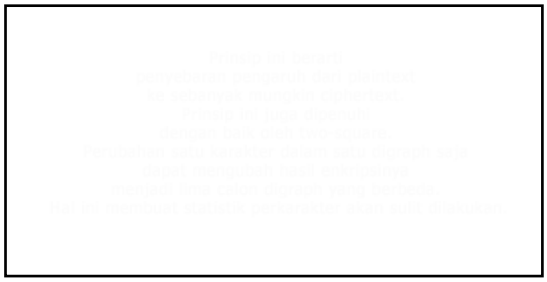


Gambar 12: pengaturan *opacity* untuk 'enkripsi'

4. Klik ctrl+E untuk menyatukan gambar lalu disimpan

Hasil yang didapatkan adalah gambar yang tersamar sehingga keseluruhan tampak seperti warna putih. Hal ini dikarenakan mata manusia tidak mampu meraba beda warna yang ada. Namun, *photoshop* masih dapat mendeteksi perbedaan warna antara keduanya sehingga inilah yang dapat dimanfaatkan untuk proses 'dekripsi'-nya nanti.

1. 

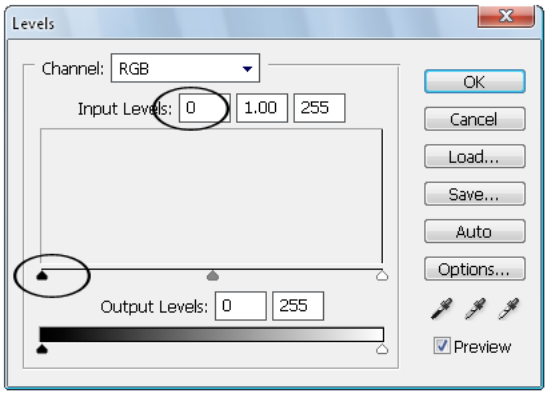
2. 

Gambar 13: Contoh gambar yang sesungguhnya (1) dan gambar yang telah diubah *opacity*-nya (2)

Dapat dilihat dari gambar di atas bahwa gambar tersamarkan dengan baik. Gambar yang seolah tampak putih sempurna itulah yang dapat dikirim-terimakan untuk nantinya didekripsikan.

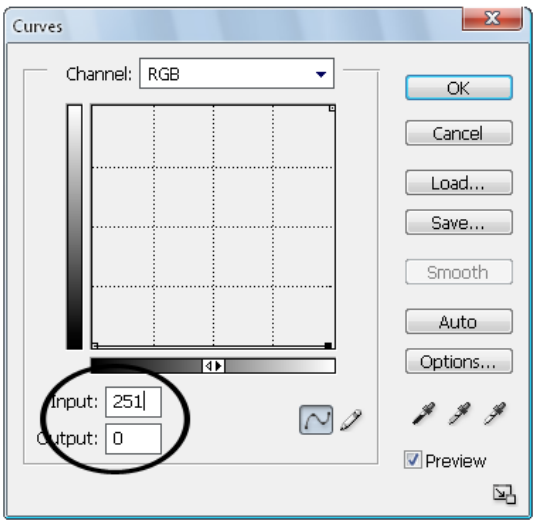
Sementara itu, cara 'dekripsi' gambar ini juga sangat mudah. Yakni sebagai berikut:

1. Buka *file* gambar yang ingin didekripsikan
2. Buka jendela *levels* (*image->adjustment->levels*)

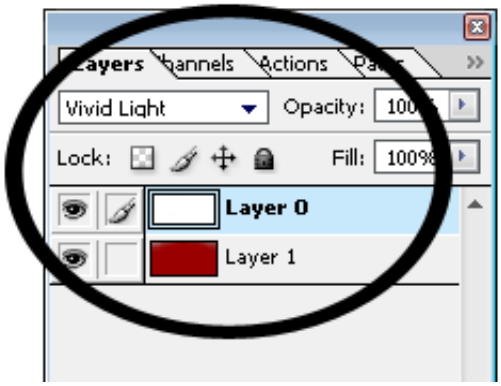


Gambar 14: Pengaturan *levels* untuk 'dekripsi' gambar

3. Geser anak panah yang dilingkari ke kanan atau ubah input level hingga ke arah maksimal (253). Jumlah ini sebetulnya dapat disesuaikan bergantung pada tingkat kenyamanan mata. Semakin tinggi jumlah yang dimasukkan, semakin nyata perbedaan warna yang tadi tersamarkan dengan latar belakang
4. Selain menggunakan *levels*, dapat juga menggunakan *tools* lain. Misalnya dengan menggunakan *curves* (*image-> adjustment->* curves) untuk mengubah *setting input* ke 251 dan *output* menjadi 0), atau menambahkan layer lain di bawah layer tersebut dan mengisinya dengan warna selain putih, kemudian mengubah layer gambar yang ingin di'enkripsi' tersebut dari *Normal* ke *Vivid Light*.

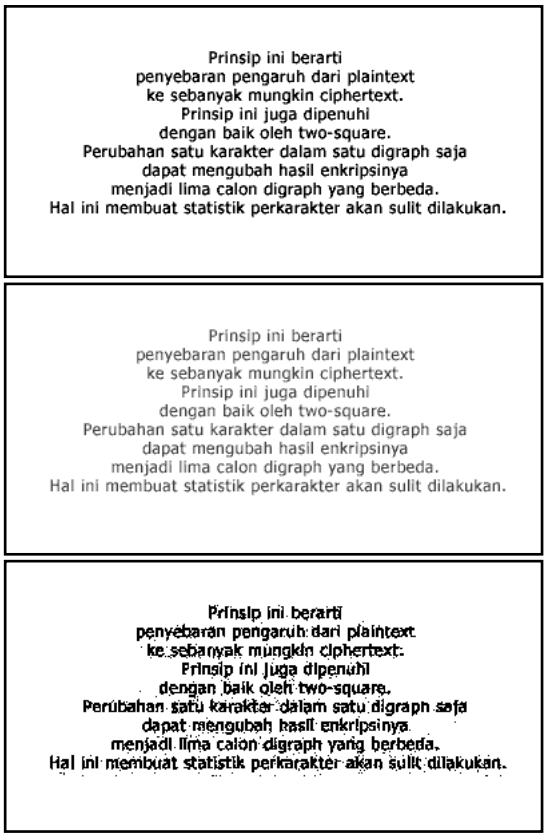


Gambar 15: Pengaturan *curves* untuk 'dekripsi' gambar



Gambar 16: Pengaturan *layers* untuk 'dekripsi' gambar. Layer 0 adalah layer gambar yang ingin di'dekripsi' dan layer 1 adalah layer tambahan

Hasil dari ketiga cara tersebut dapat dilihat perbandingannya sebagai berikut:

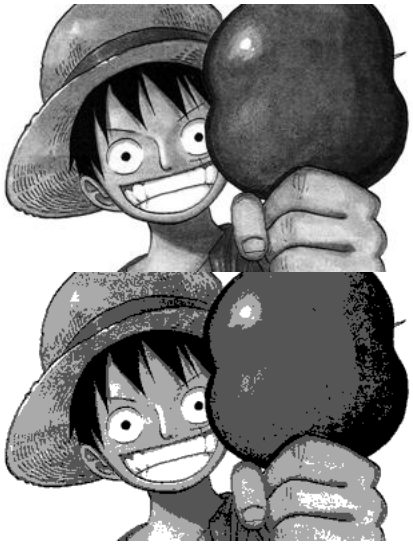


Gambar 13: Hasil 'dekripsi' *file* pada gambar 13

Yang teratas adalah penggunaan *levels* untuk 'dekripsi', disusul dengan penggunaan *curves*, dan yang terakhir menggunakan teknik penyusunan layer dengan layer tambahan berwarna hitam pekat (#000000). Dari gambar di atas, tampak yang paling mendekati aslinya adalah yang menggunakan *levels*. Tingkat kecerahannya paling baik. Tidak terlalu buram dan tipis seperti dengan menggunakan *curves* namun juga tidak terlalu tebal dan mengandung bintik-bintik *noise* seperti ketika menggunakan teknik pengaturan *layer*.

Berdasarkan hasil percobaan di atas, berikutnya akan dipilih *levels* untuk pengetesan 'enkripsi'-'dekripsi' gambar.

Berikut adalah hasil percobaan pada jenis gambar lain. Gambar yang digunakan masih dari *manga* One Piece karya Eiichiro Oda volume 62.



Gambar 14: Gambar asli dan gambar hasil 'dekripsi' pada file gambar hitam putih

Gambar 14: Gambar asli dan gambar hasil 'dekripsi' pada file gambar berwarna

Dari contoh-contoh di atas bisa dikatakan hasil yang berbeda tidak terlalu jauh berbeda. Di contoh yang pertama misalnya, gambar berupa teks, tulisan masih bisa dibaca dengan jelas. Yang berbeda adalah warna tulisan yang semakin terasa jelas dan lebih tebal dibandingkan dengan gambar aslinya.

Di contoh berikutnya, pada file berupa gambar, dapat dikatakan bahwa hasilnya tidak sebaik jika menggunakan penyamaran pada tulisan. Hasil yang lumayan didapatkan jika menggunakan gambar hitam putih. 'Dekripsi' gambar berwarna menghasilkan warna yang terlalu mencolok. Hal ini sebetulnya tergantung dari besar input yang dimasukkan saat mengatur *levels*. Semakin tinggi (semakin ke kanan) maka semakin nyata dan mencolok warna yang dihasilkan pada gambar.

Gradasi untuk gambar yang di'dekripsi' dengan ini masih terasa belum sempurna. Namun tetap terlihat perbedaan warna dari putih, semakin gelap menuju abu-abu, hingga akhirnya menjadi hitam. Demikian juga halnya pada *file* gambar dengan warna, memiliki warna yang cukup kaya untuk dapat dikenali warna-warna setiap elemen. Tidak hanya warna dasar saja, tapi juga warna sekunder, tersier, dan seterusnya. Pergeseran warna masih agak kasar dan *saturation* berlebihan.

IV. ANALISIS PERBANDINGAN

Prinsip Penyandian Shannon sebetulnya adalah dasar untuk pembangunan algoritma blok yang kuat. Namundua prinsip ini juga dapat digunakan untuk menganalisis perbandingan kekuatan dua cara penyembunyian pesan tersebut. Ditilik dari Prinsip Penyandian Shannon, untuk *confusion* dan *diffusion*, jelas teknik kriptografi visual lebih unggul karena:

1. Berdasarkan prinsip *confusion*, menyembunyikan hubungan plainteks dan cipherteks, kriptografi visual melakukannya dengan baik. Tiap-tiap pixel yang dibagi menjadi subpixel diperhitungkan lagi pixel yang akan dihasilkan dengan pola-pola tersebut. Unggulnya lagi, setiap *share* dengan gambar yang tidak terbaca tersebut jika disatukan akan membentuk pola yang bisa dilihat dengan mata manusia awam.
   Sementara dalam teknik penyembunyian sederhana dengan *photoshop* ini, tidak ada perhitungan statistik dan sebagainya. Semuanya murni hanya pengurangan *opacity* sedemikian rupa hingga mata manusia tidak mampu membedakan gambar yang telah pudar dengan layar.
2. Berdasarkan prinsip *difusion*, kriptografi visual juga melakukannya dengan baik. Karena setiap titik pixel mempengaruhi seperti apa *noise* yang terdapat dalam *share*. Meskipun mata manusia tidak terlalu dapat membedakannya (semuanya tampak hanya seperti *noise*), namun jika dibandingkan, setiap perubahan menghasilkan pola *noise* yang berbeda.
   Sementara lagi-lagi, dalam teknik penyembunyian sederhana menggunakan *photoshop*, gambar seperti apa pun akan menghasilkan gambar berwarna putih yang sama. Perubahan setiap pixel atau satu gambar utuh pun tidak dapat dideteksi dengan mata manusia normal.

Akan tetapi, analisis perbandingn dengan Prinsip Penyandian Shannon ini dirasa kurang. Prinsip Penyandian Shannon hanya memperhatikan faktor keamanan agar tidak mudah diketahui dan dicari dekripsinya. Prinsip ini tidak memperhitungkan faktor-faktor lain misalnya tingkat kecurigaan, kualitas hasil gambar akhir, kemudahan enkripsi-dekripsi dan sebagainya. Ditambah lagi, teknik penyembunyian gambar dengan *photoshop* memang bukan kriptografi murni. Melainkan hanya sebuah cara untuk menyembunyikan gambar dan nanti dapat di'dekripsi' kembali *seolah-olah* merupakan kriptografi.

1. Tingkat kecurigaan

Berdasarkan survey yang dilakukan terhadap orang awam (dalam hal ini tidak paham kriptgrafi), didapatkan kesimpulan bahwa gambar dengan *noise* (*share* hasil enkripsi kriptografi visual) lebih menimbulkan rasa ingin tahu dan kecurigaan memiliki makna tertentu daripada gambar dengan warna putih polos.

Artinya, kriptografi visual memiliki tingkat kecurigaan yang lebih besar dan lebih memiliki kemungkinan untuk dilakukan serangan. Meski orang tanpa pengetahuan kriptografi yang cukup atau tanpa kemampuan grafis yang cukup mungkin juga tidak mengetahui cara melihat gambar asli yang dimaksud.

2. Kemudahan enkripsi

Enkripsi kriptografi visual terhitung rumit. Hal ini karena memperhitungkan pixel-pixel yang membentuk suatu titik warna. Enkripsinya harus mempergunakan komputer dengan program tertentu. Photoshop sebetulnya juga dapat digunakan untuk enkripsi kriptografi visual, namun langkah yang disediakan terhitung banyak dan tidak mudah untuk diikuti. Dibandingkan dengan metode penyembunyian sederhana, 'enkripsi'-nya jauh lebih unggul. Hanya dengan satu langkah mudah untuk menurunkan *opacity* lalu gambar akan tersamarkan. Sehingga lagi-lagi di sini metode ini lebih unggul dibandingkan kriptografi visual.

3. Kemudahan dekripsi

Jika 'tidak-menggunakan-komputer' dapat dikatakan sebagai kelebihan, maka kriptografi visual menjadi lebih unggul. Keistimewaan kriptografi visual memang supaya pendekripsi tidak perlu menggunakan komputer, hanya tinggal menumpuk layar *share* yang ditransparansi sedemikian rupa dan nanti hasilnya akan tampak secara langsung.

Sementara itu, seperti yang disebutkan di bagian III mengenai cara 'dekripsi', metode penyembunyian sederhana dengan pemanfaatan *Photoshop* ini memang harus menggunakan komputer dengan bantuan perangkat lunak serupa *Photoshop* yang telah ter-*install* atau perangkat lunak sejenis misalnya GIMP. Meskipun proses 'dekripsi' sendiri tidak terhitung rumit, namun masih kalau unggul dibanding kriptogravi visual yang tidak membutuhkan *tool* apa-apa.

4. Kualitas hasil 'dekripsi'

Gambar-gambar yang disajikan dalam bagian II dan III telah menunjukkan sendiri bahwa metode penyembunyian dengan *Photoshop* ini memiliki hasil dekripsi yang lebih baik setelah dilakukan percobaan pada *file* gambar berisi teks, gambar hitam putih, dan gambar berwarna. Pada hasil dekripsi kriptografi visual, semakin kecil gambar dan semakin kompleks unsur yang ada di salamnya, semakin sulit terbaca hasil dekripsinya. Hasil dekripsi akan kehilangan sejumlah unsur penting dan sangat sulit sekali meraba gambar apa aslinya.

Unsur penting pada gambar yang dimaksud misalnya garis, teks, bayangan, gradasi, hingga warna. Kriptografi jauh lebih miskin warna dibandingkan dengan teknik

penyembunyian gambar sederhana dengan *Photoshop* ini. Begitu pula bayangan yang nyaris tidak tampak, teks yang tidak terbaca dan lain sebagainya.

Dari analisis perbandingan di atas, dapat dilihat bahwa untuk kriptografi visual sebetulnya adalah langkah yang baik untuk menyembunyikan gambar karena memenuhi Prinsip Penyandian Shannon. Akan tetapi setelah ditinjau berbagai jenis kekurangannya, metode ini dirasa kurang, dibandingkan dengan trik menyembunyikan gambar sederhana tadi. Masalah yang paling besar adalah gambar asli yang jauh dari gambar setelah *share* ditumpuk sehingga makna yang dimaksudkan mungkin sekali tidak sampai. Algoritma sebaik apa pun rasanya akan percuma jika hasilnya perbedaan pemahaman antara pihak pengenkripsi dan pendekripsi.

Oleh karena itu, metode penyembunyian gambar dengan *Photoshop* dianggap lebih unggul meskipun tidak sesuai dengan Prinsip Penyandian Shannon. Paling tidak sampai ditemukan metode untuk meminimalisasi *noise* yang terdapat dalam hasil dekripsi dan memperbaiki jumlah warna yang ada.

IV. KESIMPULAN

Kesimpulan yang dapat diambil dari makalah ini adalah sebagai berikut:

1. Selain kriptografi visual, terdapat banyak metode lain yang dapat digunakan untuk menyembunyikan gambar. Salah satunya adalah dengan bantuan *Adobe Photoshop.*
2. Kriptografi visual memiliki kelemahan dan kekurangan sendiri dibandingkan dengan metode sederhana untuk penyembunyian gambar. Kelemahan utamanya yaitu *noise* yang membuat gambar hasil dekripsi sulit dimengerti membuat kriptografi visual sebaiknya tidak menjadi pilihan untuk penyembunyian gambar.
3. Metode sederhana dengan bantuan *Photoshop* layak dicoba untuk penyembunyian gambar.

V. REFERENSI

[1] Munir, Rinaldi. (2006). "Diktat Kuliah IF5054 Kriptografi", Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika , InstitutTeknologi Bandung.

[2] Play Color Cipher and Visual Cryptography (http://www.decisionstats.com/play-color-cipher-and-visual-cryptography/, waktu akses 11 Mei 2012, pukul 17.00)

[3] Visual Cryptography (http://www-sec.uni-regensburg.de/vc/, waktu akses 11 Mei 2012 pukul 21.00)

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 14 Mei 2012

ttd

Risalah Widjayanti
13509028